# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-282667
(43)Date of publication of application : 15.10.1999

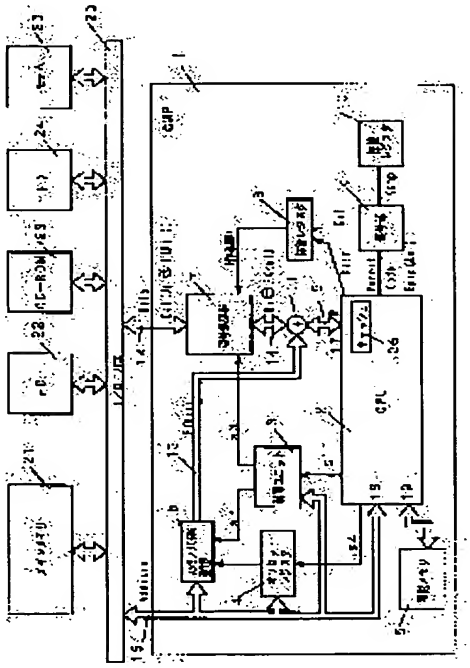
(51)Int.Cl. G06F 9/06
G06F 12/14
G06F 15/78
G09C 1/00
H04L 9/14
H04L 9/32

(21)Application number : 10-103958
(22)Date of filing : 31.03.1998

(71)Applicant : NAKAMICHI CORP
(72)Inventor : SUEMATSU TOSHINARI

## (54) MICROPROCESSOR HAVING CIPHER PROCESSING FUNCTION OF MULTIPLE KEY SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain the data which can be decoded by only a CMP and to prevent the disadvantage caused by the leakage of data by enciphering and decoding a data group by means of a job key that is enciphered by a secret key proper to the CMP.
SOLUTION: A CMP 1 has its proper secret key Ksmp that is stored in its built-in storage register 10 and to be used for the decoding jobs of a decoding part 9. An offset register 4 receives a fetch signal s4 which is outputted from a CPU 2 and outputs the head address data to a scramble code generator 6. The generator 6 outputs a scramble code F(Re) generated from the head address data and the address data inputted from an address bus 16 to an adder 11 via a signal path 13. The adder 11 performs an exclusive OR operation between the code F(Re) and the data which are inputted from one of data paths 14 or 15. Then the adder 11 outputs the result of its exclusive OR operation to the other one of paths 14 and 15 to carry out the scramble and descramble operations.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－282667

(43)公開日　平成11年(1999)10月15日

| (51)Int.Cl.[6] | | 識別記号 | FI | | |
|---|---|---|---|---|---|
| Ｇ０６Ｆ | 9/06 | ５５０ | Ｇ０６Ｆ | 9/06 | ５５０Ａ |
| | | | | | ５５０Ｅ |
| | 12/14 | ３２０ | | 12/14 | ３２０Ｂ |
| | 15/78 | ５１０ | | 15/78 | ５１０Ｇ |
| Ｇ０９Ｃ | 1/00 | ６２０ | Ｇ０９Ｃ | 1/00 | ６２０Ｚ |

審査請求　未請求　請求項の数６　ＦＤ　（全 20 頁）　最終頁に続く

(21)出願番号　特願平10－103958

(22)出願日　平成10年(1998)３月31日

(71)出願人　000110468
ナカミチ株式会社
東京都小平市鈴木町１丁目153番地

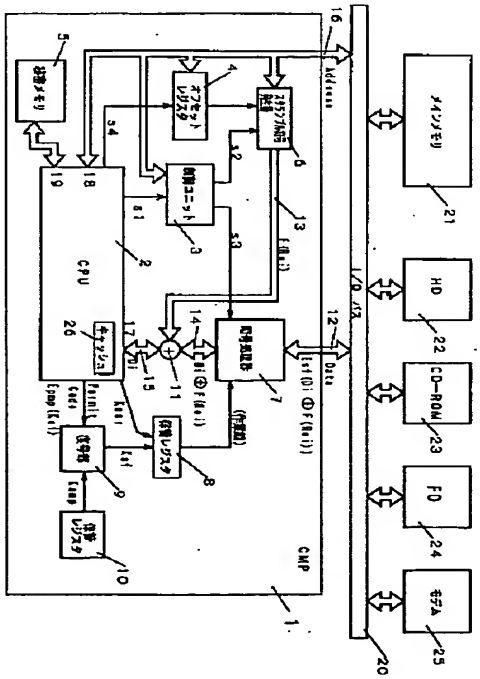
(72)発明者　末松　俊成
東京都小平市鈴木町１丁目153番地　ナカミチ株式会社内

(54)【発明の名称】　多重鍵方式の暗号処理機能を有するマイクロプロセッサ

(57)【要約】

【目的】鍵で暗号化したソフトウエアを特定のコンピュータでのみ使用可能にし、且つこの暗号化ソフトウエアは、例えばＣＤ－ＲＯＭのように同一の複製品を市場で販売可能とする。一方、暗号化ソフトウエアを復号する場合、暗号化したコンピュータでのみ復号化が可能とし、データの漏洩による不利益を防止する。

【構成】ソフトウエアに用意された作業鍵によって暗号された暗号化ソフトウエアと、後述する秘密鍵に対応する公開鍵で前記作業鍵を暗号化した暗号コードとを別々に入手し、マイクロプロセッサに固有の秘密鍵を外に読み出し不可に保存する記憶手段と、この秘密鍵で前記暗号コードを復号化して前記作業鍵を生成する復号手段と、この作業鍵を保持する記憶手段と、この作業鍵によって前記暗号化ソフトウエアを復号化する復号手段とを有するマイクロプロセッサ。



1

【特許請求の範囲】

【請求項１】暗号化されたソフトウエアを復号化する第１の復号手段と、

前記第１の復号手段による復号化を行うための第１の鍵を保存する第１の記憶手段と、

暗号化された前記第１の鍵を復号化して前記第１の記憶手段に保存する第２の復号手段と、

前記第２の復号手段による復号化を行うための第２の鍵を保存する第２の記憶手段とを有することを特徴とする１チップで構成された多重鍵方式の暗号処理機能を有するマイクロプロセッサ。

【請求項２】前記第１の鍵と前記第１の記憶手段とをそれぞれ複数としたことを特徴とする請求項１に記載の多重鍵方式の暗号処理機能を有するマイクロプロセッサ。

【請求項３】前記第２の鍵を復号化又は暗号化により生成することを特徴とする請求項１に記載の多重鍵方式の暗号処理機能を有するマイクロプロセッサ。

【請求項４】ソフトウエアに用意された第３の鍵によって暗号化された暗号化ソフトウエアを復号化する１チップで構成された多重鍵方式の暗号処理機能を有するマイクロプロセッサであって、

前記マイクロプロセッサ固有の第４の鍵を該マイクロプロセッサ外に読み出し不可に保存する第３の記憶手段と、

前記第４の鍵に対応する第５の鍵で前記第３の鍵を暗号化した暗号コードを前記第４の鍵で復号化して前記第３の鍵を生成する第３の復号手段と、

前記第３の鍵を保持する第４の記憶手段と、

前記第３の鍵によって前記暗号化ソフトウエアを復号化する第４の復号手段とを有することを特徴とする多重鍵方式の暗号処理機能を有するマイクロプロセッサ。

【請求項５】ソフトウエアを暗号化／復号化する１チップで構成された多重鍵方式の暗号処理機能を有するマイクロプロセッサであって、

第６の鍵を暗号化した第７の鍵を生成する第１の暗号化手段と、

前記第７の鍵を保存する第５の記憶手段と、

前記第１の暗号化手段による暗号化を行うための第８の鍵を保存する第６の記憶手段と、

前記第７の鍵によって前記ソフトウエアを暗号化／復号化するための暗号化／復号化手段とを有することを特徴とする多重鍵方式の暗号処理機能を有するマイクロプロセッサ。

【請求項６】ソフトウエアに用意された作業鍵によって暗号化された暗号化ソフトウエアを復号化する１チップで構成された多重鍵方式の暗号処理機能を有するマイクロプロセッサであって、

前記マイクロプロセッサ固有の秘密鍵を該マイクロプロセッサ外に読み出し不可に保存する第７の記憶手段と、

前記秘密鍵に対応する公開鍵で前記作業鍵を暗号化した暗号コードを前記秘密鍵で復号化して前記作業鍵を生成する第５の復号手段と、

前記作業鍵を保持する第８の記憶手段と、

前記作業鍵によって前記暗号化ソフトウエアを復号化する第６の復号手段とを有することを特徴とする多重鍵方式の暗号処理機能を有するマイクロプロセッサ。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号処理機能を有するマイクロプロセッサに関し、特に暗号化されたソフトウエアを復号化する際に、複数の鍵を用いて行うマイクロプロセッサに関する。

【０００２】

【従来の技術】従来のこの種の暗号化方式に於いては、１種類の鍵でソフトウエアの復号化を行う方式のコンピュータシステムが提案されている。

【０００３】

【発明が解決しようとする課題】従来方式の場合、同じ内容のソフトウエアであっても、コンピュータシステム毎に異なる鍵で暗号化する必要があるため、例えばＣＤ－ＲＯＭのような同一の複数媒体を市場に投入出来ない。また、あるコンピュータシステムがソフトウエアを暗号／復号する場合、鍵が限定されるために解読されやすく、安全上に問題があった。

【０００４】

【課題を解決するための手段】ソフトウエアに用意された例えば作業鍵によって暗号化された暗号化ソフトウエアと、例えば後述する秘密鍵に対応する公開鍵で前記作業鍵を暗号化した暗号コードとを別々に入手し、例えばマイクロプロセッサに固有の秘密鍵を外に読み出し不可に保存する記憶手段と、この秘密鍵で前記暗号コードを復号化して前記作業鍵を生成する復号手段と、この作業鍵を保持する記憶手段と、この作業鍵によって前記暗号化ソフトウエアを復号化する復号手段とを有するマイクロプロセッサによって前記暗号化ソフトウエアを復号化する。

【０００５】また、例えばユーザーが設定した作業鍵を暗号化し、暗号化された作業鍵を生成する暗号化手段と、暗号化された作業鍵を保存する記憶手段と、この暗号化を行うための例えばこのマイクロプロセッサに固有の秘密鍵を保存する記憶手段と、前記暗号化された作業鍵によって前記ソフトウエアを暗号化／復号化するための暗号化／復号化手段とを有するマイクロプロセッサによって前記ソフトウエアを暗号化／復号化する。

【０００６】

【発明の実施の形態】図１は、本発明の一実施例を示す構成図で、図中１は、暗号化機能を有するマイクロプロセッサ（以下ＣＭＰと称す）であり、１チップで構成されている。この中の２は中央演算処理装置（以下ＣＰＵと称す）を示し、３は制御ユニットを示す。この制御ユ

ニット３は、ＣＰＵ２からの指令信号ｓ１を入力して、スクランブル符号発生器６の動作のオン、オフを指令する動作指令信号ｓ２と暗号処理器７の暗号化／復号化機能の実行、停止の各動作を指令する動作指令信号ｓ３とをそれぞれ出力する。

【０００７】このCMP１は、固有の秘密鍵Ksmpを所有する。これは内蔵の保管レジスタ１０に保管され、後述するごとくこの秘密鍵に対応する公開鍵Kpmpで作業鍵Ksfを暗号化したパーミットコードを復号部９で復号化するための鍵となる。この秘密鍵Ksmpは、CMPの製造元のみが知るもので、CMPの外に現れないようにされてユーザー等の第３者が知ることは出来ず、逆に公開鍵Kpmpは、CMPの入手時にユーザーに知らされて全ての人が知り得るものである。ここで復号化された作業鍵Ksfは、保管レジスタ８に保管される。

【０００８】CMP１につながるアドレスバス１６とデータバス１２は、Ｉ／Ｏバス２０を介してメインメモリ２１、ハードディスク２２、CD－ROM２３、フロッピディスク２４の各ドライブ、及びモデム２５の各入出力ポートにつながっている。

【０００９】一方CMP１内部において、アドレスバス１６は、ＣＰＵ２のアドレスポート１８、制御ユニット３、オフセットレジスタ４、及びスクランブル符号発生器６につながり、データバス１２は、暗号処理器７、加算回路１１を介してＣＰＵ２のデータポート１７につながっている。

【００１０】オフセットレジスタ４は、ＣＰＵ２から出力される取り込み信号ｓ４を受信し、後述するようにＣＰＵ２がメインメモリ２１との間で読み書きする際のデータの先頭位置を示す先頭アドレスデータを取り込んでメモリし、この先頭アドレスデータをスクランブル符号発生器６に出力する。スクランブル符号発生器６は、後述するようにこの先頭アドレスデータとアドレスバス１６から入力するアドレスデータをもとに生成したスクランブル符号Ｆ(Re)を信号経路１３を介して加算器１１に出力する。

【００１１】加算器１１は、このスクランブル符号Ｆ(Re)とデータ経路１４，１５の一方のデータ経路から入力するデータの排他論理和演算を行い、その結果を他方のデータ経路に出力することによりこれ等のデータのスクランブルとデスクランブルを実行する。

【００１２】ここで、図１の各部で、データに対して行う暗号化、復号化、及びデータスクランブルの各内容について更に説明する。ここで使用される共通鍵方式と公開鍵方式の２つの暗号化方式は一般的なものであり、その詳細な説明は省略するが、本文で用いるそれらの記述方法について説明する。

【００１３】共通鍵方式では、データＤを暗号化するときに秘密鍵Kabを用い、これによって暗号化されたデータをEab（D）と標記する。この場合、秘密鍵Kabがあれば、Eab（D）と記述された暗号化データを復号化して再びデータＤを取り出すことができる。

【００１４】一方、公開鍵方式では、データＤを暗号化するときに、公にされた公開鍵Kpabを用いて行ない、これによって暗号化された暗号化データをEpab（D）と標記する。この場合、この暗号化データの解読はこの公開鍵Kpabに対応する秘密鍵Ksabによってのみ行なうことが出来る。

【００１５】即ち、共通鍵方式では、一つの秘密鍵Kabによってデータの暗号化と復号化を行なうが、公開鍵方式では、公にする公開鍵Kpabではデータの暗号化のみが可能であって、その復号化には秘密鍵Ksabを用いて行なう。

【００１６】次に、アドレスによって行なわれるデータスクランブルについて、その一例を示す本実施例の原理を説明する。簡単のため、データＤが記憶手段に書き込まれる際には１バイト単位で行なわれ、各単位毎にアドレスAdを対応させて処理するものとする。また暗号化スクランブルされるデータは、メインメモリ２１内の連続した領域におかれ、この一連の連続するデータの集合をデータ群と呼ぶことにする。１つのプログラムやデータは、通常１つ以上のデータ群で構成されるが、スクランブルは、データ群毎に処理される。

【００１７】以降では説明を簡単にするため、プログラムやデータは、１データ群で構成されるものと仮定する。そこで、データ群ＤＸを１バイトデータのデータ列、D1, D2……DNの集合として標記し、アドレス群AdXをこれ等の各１バイトデータに対応して付されるアドレスAd1，Ad2……AdNの集合として標記する。

【００１８】従って、この連続データの各アドレスAdi（i=1, 2, ……N）は、その先頭アドレスをToとし（通常はTo＝Ad1）、この先頭アドレスからの相対位置を示す相対アドレスをReiとしたとき、Adi＝To＋Reiとして表せる。図１のオフセットレジスタ４は、この先頭アドレスToをメモリするものである。

【００１９】一方、スクランブル符号発生器６は、逐次入力するアドレスAdiと先頭アドレスToとからこの相対アドレスReiを算出し、この値に１対１で対応するも、規則性を示さない１バイトのスクランブル符号Ｆ(Rei)を発生する。このようにして生成されるスクランブル符号の集合をＦ(ReX)と標記する。加算器１１は、データ経路１４，１５の内、一方から逐次入力する１バイトのデータと、このデータのアドレスに対応して入力するスクランブル符号Ｆ(Rei)との排他論理和データを他方のデータ経路に出力する。

【００２０】従って、例えば、ＣＰＵ２から出力されるデータD1がメインメモリ２１にメモリされる時の一過程を説明すると、この時にデータD1、例えば（10010001）が出力されると共に、このデータの番地を指定するアドレスAd1が出力される。加算器１１は、このデータを

入力すると共に、この時の指定アドレスから算出された相対アドレスRelに対応して発生したスクランブル符号F(Rel)、例えば(11001100)を入力し、これ等の排他論理和(01011101)を暗号処理器７に出力する。

【００２１】このように、データDiとスクランブル符号F(Rei)との排他論理和によってスクランブルされたデータを（Di(+)F(Rei)）と記述して図１中に示す。従って、この図からもわかるように、データ経路１４はスクランブルされたデータの経路となる。

【００２２】次に、スクランブルされたデータを解除する例として、ＣＰＵ２が上記したデータD1を読み込む時の一過程を考えてみる。この時、このデータD1を読み出すためのデータとして上記アドレスAd1が出力され、これに伴ってスクランブル符号F(Rel)がスクランブル符号発生器６から出力されことが理解される。

【００２３】従って加算器１１は、この時データ経路１４に表れるスクランブルされた（D1(+)F(Rel)）のデータ列(01011101)とスクランブル符号F(Rel) のデータ列(11001100)との排他論理和(10010001)、即ちデスクランブルされる前の元のデータD1をＣＰＵ２に出力する。

【００２４】このように、加算器１１は、データD1とこれに対応するスクランブル符号F(Rel) との排他論理和をとってスクランブルされたデータ（D1(+)F(Rel)）を形成し、逆にこのデータ（D1(+)F(Rel)）とスクランブル符号F(Rel) との排他論理和をとってデスクランブルされる前の元のデータD1を生じるべく動作することが理解される。

【００２５】次に、図２の実行準備フローに従って、暗号化され更にスクランブルされたアプリケーションソフトを入手し、その実行に際してＣＰＵ２内への読み込みを可能にするまでの準備過程について主に説明する。この時のアプリケーションソフトをデータ群DapXで示すと、上記した如くこのデータ群DapXに対応して生成されるスクランブル符号F(ReX)でスクランブルされ、共通鍵方式の作業鍵Ksf２で暗号化されたアプリケーションソフトは、Esf２（DapX(+)F(ReX)）で示される。

【００２６】尚、この作業鍵Ksf２は、前記した共通鍵方式の秘密鍵に相当するものであるが、公開鍵方式の秘密鍵と区別するために以後作業鍵と称すことにする。また、ここで設定される作業鍵Ksf２は、このアプリケーションソフト供給元がこのソフト専用に用意するもので、この作業鍵Ksf２で他のアプリケーションソフトを解読することは出来ない。

【００２７】この暗号化されたアプリケーションソフトEsf２（DapX(+)F(ReX)）は、図１０に示すように後述するパーミットコードを管理するための暗号化されていない起動処理プログラムと一対にされた配給ソフトとしてソフト供給元から供給される。

【００２８】図示しない入力手段により所望のアプリケーションソフトの実行指令を受けると（ステップ１）、ＣＰＵ２は、先ずスクランブル符号発生器６の出力を停止すると共に、暗号処理器７の復号機能を停止するための指令信号ｓ１を出力する（ステップ２）。そして次のステップ３で、この配給ソフトがメインメモリ２１にロードされ、更に起動処理プログラムがＣＰＵ２に読み込まれて実行される。

【００２９】この暗号化されたアプリケーションソフトEsf２（DapX(+)F(ReX)）がメインメモリにロードされる際に、メインメモリ２１に指定される先頭アドレスＴｏはその管理状況によって変わるが、前記したようにそれに続くアドレスは連続的に指定されるため、この時の先頭アドレスToからの相対位置を示す相対アドレス群は、スクランブル時に用いられた相対アドレス群ReXと同じデータとなる。

【００３０】この配給ソフトの供給手段としてはハードディスク２２、ＣＤ－ＲＯＭ２３、フロッピーディスク２４及び、モデム２５等による方法が考えられるが、その方法は一般的に行なわれている方法を採用できるため、ここでその詳しい説明は省略する。

【００３１】続くステップ４から１０のステップは、いま実行された起動処理プログラムに従って実行され、次のステップ４では、この暗号化アプリケーションソフト専用の作業鍵Ksf２を公開鍵Kpmpで暗号化したパーミットコードEpmp（Ksf２）がハードディスク２２に既にメモリされているかを確認する。この公開鍵Kpmpは、上記したように図１のＣＭＰ１固有の秘密鍵Ksmpに対応するもので、この秘密鍵Ksmpのみによって復号することが可能となる。

【００３２】従って、この場合のパーミットコードEpmp（Ksf２）は、公開鍵で作業鍵を暗号化したものであり、アプリケーションソフト供給元が、ＣＭＰ１のユーザーから公開鍵Kpmpを入手して作成する。ステップ４でこのパーミットコードの存在が確認できないと、ＣＭＰ１のユーザーは何らかの方法でソフト供給元からこれを入手し（ステップ５）、このアプリケーションソフトの専用ファイルにパーミットコードを入力し、ハードディスク２２にこれを保存する（ステップ６）。この様にパーミットコードの入力保存は、通常は暗号化されたアプリケーションソフトと対になったこの起動処理プログラムによって行なわれる。

【００３３】次に、パーミットコードEpmp（Ksf２）の存在を確認するとこれを読み込み（ステップ７）、内蔵の保管レジスタ１０に保管している秘密鍵Ksmpでこれを復号化して得た作業鍵Ksf２を保管レジスタ８に保管する（ステップ９）。

【００３４】次にＣＰＵ２は、スクランブル符号発生器６の出力を再開し、暗号処理器７の暗号化／復号化機能を起動するための指令信号ｓ１を出力する（ステップ１０）。そしてステップ１１に至り、必要に応じてこのメ

インメモリ２１に保管された暗号化されたアプリケーションソフトEsf２（DapX(+)F(ReX)）がＣＰＵ２へ読み込まれて実行される。

【００３５】従って、この時この暗号化されたアプリケーションソフトEsf２（DapX(+)F(ReX)）は、暗号処理器７によって作業鍵Ksf２で復号化されて（DapX(+)F(ReX)）となる。また上記のごとく、この時のアドレスデータから生成されるスクランブル符号はF(ReX)であり、加算器１１は、これ等の排他論理和を行なってデスクランブルされたアプリケーションソフトDapXをＣＰＵ２のデータポート１７に出力する。

【００３６】以上のようにして、アドレススクランブルと暗号化されたアプリケーションソフトがＣＰＵ２に読み込まれる。このようにして暗号化されたアプリケーションソフトとパーミットコードの組合せにより、下記の長所をあげることができる。

【００３７】長所

１．ソフト供給元は、供給するソフトを所定のCMPでのみ利用させることが出来る。CMPの秘密鍵Ksmpがその外部に現れることがなく、ユーザーを含む第３者によってチェック出来ないため。

２．暗号化されたアプリケーションソフトをＣＤ－ＲＯＭ等の複製可能な媒体により市場に出すことができる。同種のアプリケーションソフトは、同じ作業鍵で暗号化されるため。

３．異種のアプリケーションソフトは、それぞれ専用の作業鍵で暗号化されなければならないが、アプリケーションソフトの種類だけ異なる作業鍵を用意すればよい。

【００３８】次に、ユーザーによって作成され、一旦メインメモリ２１に保存したデータを、暗号化して再度メインメモリ２１に保存しなおす過程を図３のフローチャートを用いて説明する。この場合、このデータを作成する段階では、データの暗号化は行なわれないものとする。

【００３９】このプログラムが起動すると、上記したようにユーザーによって作成されたデータ群DsXが暗号化されないままメインメモリ２１に保管される（ステップ２１）。次にＣＰＵ２は、キーボード等の入力手段（図示せず）から入力するユーザーからの指示に基づいてこのデータ群DsXを共通鍵方式で暗号化するための作業鍵Kusrを決定し（ステップ２２）、これを保管レジスタ８に出力して保管する。

【００４０】次にＣＰＵ２は、メインメモリ２１のデータ群DsXを読み込むために、スクランブル符号発生器６の出力を停止すると共に、暗号処理器７の機能を一時停止するための指令信号ｓ１を出力する（ステップ２５）。この時データ群DsXはそのままＣＰＵ２に読み込まれるが１バイト毎にアドレス指定されて読み込まれ（ステップ２６）、この段階では最初の１バイト分のデータDs1がＣＰＵ２に読み込まれる。尚、データ群DsXは、１バイトデータDs1, Ds2, ……DsNの集合として標記する。

【００４１】次にＣＰＵ２は、スクランブル符号発生器６の出力を再開し、暗号処理器７の復号化機能を起動するための指令信号ｓ１を出力する（ステップ２７）。この状態でＣＰＵ２は、取り込んだ１バイト分のデータDs1を再度メインメモリ２１に書き込む。

【００４２】この書き込み過程で、先ずこのデータの番地を指定するアドレスに対応してスクランブル符号発生器６から出力されるスクランブル符号F(Re1)と、このデータDs1との排他論理和（Ds1(+)F(Re1)）によるアドレススクランブルが行なわれ、これがデータ経路１４に現れる（ステップ２８）。尚、スクランブル符号F(Re1)は、上記したデータ群DsXの各１バイトデータに対応して生成されるスクランブル符号F(Re1), F(Re2), ……F(ReN)の１番目に相当し、これ等の集合をF(ReX)と標記する。

【００４３】更にこのデータ（Ds1(+)F(Re1)）は、暗号処理器７によって作業鍵Kusrで暗号化され(ステップ２８)、Eusr（Ds1(+)F(Re1)）の状態でメインメモリ２１に書き込まれる。次に、再びステップ２４に戻って、暗号化するデータ群DsXが終了するまで１バイトづつ同様の暗号化処理が繰り返される。

【００４４】そして、処理するデータDsXがなくなった段階でステップ３０に至り、スクランブル符号発生器６の出力停止と、暗号処理器７の暗号化機能停止のための指令信号ｓ１を出力する。そしてこのメインメモリ２１に書き込まれた暗号化されたデータを、HD, ＦＤ等の補助記憶装置に保存して（ステップ３１）このプログラムを終了する。

【００４５】尚、ＣＰＵ２のデータポート１７部にキャッシュメモリ２６を設けると、入出力するデータをためることができ、暗号化処理効率を上げることが出来る。即ち、ステップ２６で複数バイト、例えば１００バイト分のデータを連続して読み込み、ステップ２８でこの１００バイト分のデータを連続してスクランブル及び暗号化することによって、ステップ２５とステップ２７の各機能の切り換え行程をその分省略することが出来る。

【００４６】上記の例では、ユーザーが作成したデータを暗号化する行程を説明したが、前記したアプリケーションソフト提供元が、暗号化プログラムを作成する場合も同様の行程で処理することが出来る。アプリケーションソフトを暗号化する場合には、作成したアプリケーションソフトをデータ群DapXとしてメインメモリ２１に一旦保管し、共通鍵方式の秘密鍵として作業鍵Ksf２を設定し、上記した図３のフローに従って処理すれば、前記した暗号化されたアプリケーションソフトEsf２（DapX(+)F(ReX)）を補助記憶装置に保管することが出来る。

【００４７】また上記の実施例の場合、ステップ２で—

旦データをメインメモリに作成し、その後暗号化処理を行なうケースを示したが、データを作成する過程で直接暗号化してメモリに出力する方法も考えられる。この場合、作成したデータをメインメモリに出力する際に、その過程で１バイト毎にデータのアドレススクランブルと暗号化を行ない、メインメモリに保存するように構成すればよい。

【００４８】また前記実施例では、オフセットレジスタ４にアドレス群の先頭アドレスをメモリするように説明したが、これに限定されるものではなく、相対アドレスReiを導き出せる基準値であればよい。

【００４９】次に、ＣＭＰ１内に設けられた秘密メモリ５の働きについて説明する。このため、ソフト供給元によってその稼働時間が管理されたアプリケーションソフトを、例えば図４乃至図７の各フローチャートに従ってＣＤ－ＲＯＭ２３から取り込み、実行する場合を例に説明する。

【００５０】これ等のフローチャートの説明の前に、理解を容易にするために秘密メモリ５の働きについて、その要点を先ず説明する。図９は、秘密メモリ５に保存されるデータの内容を示すが、ここには、ＣＭＰ１が実行するｎ種類のアプリケーションソフトに１対１で対応するパスワードＰｗが保存される。

【００５１】このパスワードＰｗは、秘密メモリ５内で唯一の値であればどのような値でも良く、後述する図４のインストールフローのステップ７５では、生成される乱数によって決定される例を示す。この様にして決定されるパスワードＰｗは、秘密メモリ５内に保存されると共に、インストール実行中のアプリケーションソフトの環境設定ファイルにも保存され、後述する図５の実行フローのステップ４７で秘密値Nraの照合を行なう際に利用される。

【００５２】この秘密値Nraは、同じく図６の実行フローのステップ５７でアプリケーションソフトの実行が終了する毎に任意に発生される乱数などによって更新され、稼働可能時間を示す残量時間Treと共に実行中のアプリケーションソフトの時間データファイルDdat（Ddat＝Tre＋Nra'）としてハードディスク２２に保存される（ステップ５９）。更に、ここで更新された秘密値Nra'は、ステップ６０で秘密メモリ５内に確保された実行中のアプリケーションソフトに対応するパスワードＰｗによって同メモリ内で識別される秘密値Nraに上書きされる。尚、図５、６に示す実行フロー内において、秘密値の更新前後を区別するために、更新前の秘密値をNraで、また更新後の秘密値をNra'としてそれぞれを示す。

【００５３】このステップ６０での秘密値の更新に際しては、後述するように安全性を高めるために秘密メモリ５の更新前の秘密値Nraによる照合が行なわれる。よって、更新時には（Ｐｗ，Nra，Nra'）が用意され、パスワードＰｗによって識別された秘密メモリ５内のNraと照合のために用意したNraとが一致した場合のみ、新しい秘密値Nra'によって書換が行なわれる。このようにしてユーザー等の第３者によるNraの安易な変更を防止する。

【００５４】以上の様に秘密値Nraを秘密メモリ５に保管すると共に、時間データファイルDdatとしてハードディスク２２内に保存し、このアプリケーションソフトが実行される毎にこれ等を照合することによって、ハードディスク２２に保管されている時間データファイルDdatが第３者によって改ざんされていないかをチェックすることができる。

【００５５】例えばユーザーが、残量時間Treが十分残っている段階で時間データファイルDdatをコピーして予め別途確保しておき、このアプリケーションソフトが実行されて残量時間が僅かになった段階で、ハードディスク２２に保存される時間データファイルDdatと置き換えたとする。しかしながらこの場合、この置き換えられた時間データファイルの秘密値と秘密メモリ５に保存してある秘密値を照合することによって、このデータが正規のデータでないことが判明する。なぜならば、この場合の両者の秘密値Nraは、生成されたタイミングが異なるため、当然異なった値となっているからである。

【００５６】以上の記載から理解されるように、秘密メモリ５内のデータは、ユーザーを含め第３者によって操作出来ないようにすることが好ましい。従って、ＣＭＰ１の外部に秘密メモリ５のデータが出力されないように構成される必要がある。

【００５７】図４乃至図７の各フローチャートは、上記したように、不正なデータの改ざんを防ぐべく、秘密メモリ５を使って実施される秘密データ管理方法の全体の手順を示すもので、以下その流れを順に説明する。

【００５８】先ず、所望のアプリケーションソフトを入手してハードディスク２２にインストールし、更に必要な諸環境を初期設定するまでの流れを図４のインストールフローに従って説明する。所望のアプリケーションソフトの入手方法は種々考えられるが、このソフトが入ったＣＤ－ＲＯＭを所定のルートで入手し（ステップ７１）、インストールする例を記述する。尚、このインストールフローは、アプリケーションソフトに付随するセットアッププログラムファイルに基づいて実行されるものである。

【００５９】この場合、このＣＤ－ＲＯＭ２３がＣＤ－ＲＯＭドライブにセットされ、図示しない入力手段によってインストールの指示を受けると、そのアプリケーションソフトがハードディスク２２にインストールされる（ステップ７２）。他のインストール例として、アプリケーションソフトをモデム２５を介してダウンロードし、ハードディスク２２にインストールするようにしてもよい。

【００６０】但し、この時インストールされたアプリケーションソフトDexeXは、前記した方法でスクランブル符号Ｆ(ReX) によるアドレススクランブルと作業鍵Ksf３による暗号化が行なわれ、Esf３（DexeX(+)Ｆ(ReX)）の状態でハードディスクに保存されているものとする。

【００６１】そして次のステップ７３では、作業鍵Ksf３を確保し、保管レジスタ８にこれを保管する。そのため、このステップでは、図２のフローのステップ５からステップ９で説明したように所定の手順でソフト供給元から入手したパーミットコードEpmp（Ksf３）をハードディスク２２に保管し、復号部９で復号化する作業が含まれる。

【００６２】そして次のステップ７４では、スクランブル符号発生器６の出力を開始し、暗号処理器７の暗号化／復号化機能を起動するための指令信号ｓ１を出力する。これにより、後述するステップ８２で両機能がオフとされるまで、CMP１とメインメモリ２１等の外部記憶装置との間で入出力するデータはすべて暗号化されたものとなる。

【００６３】次のステップ７５では、前記したようにこのアプリケーションソフトに１対１で対応するパスワードＰｗ３を生成すべく乱数を発生させ、まだ秘密メモリ５内に存在しない数値であることを確認して確定し、同メモリ内にこれを確保する。そして、インストールされたアプリケーションソフトDexeXの環境設定ファイルAcfg３を作成し、この中に生成したパスワードＰｗ３を書き込んでハードディスク２２に保存する（ステップ７６）。

【００６４】次に、このアプリケーションソフトの稼働可能な残量時間Treをゼロとし（ステップ７７）、乱数を発生させて秘密値Nraを生成する(ステップ７８)。そして残量時間Treと秘密値Nraとからなる時間データファイルDdat（Ddat＝Tre＋Nra）を作成し、ハードディスク２２にこれを保存する（ステップ７９、８０）。

尚、この時作成される時間データファイルDdatは、必要に応じて一旦メインメモリ２１に保存されるが、この際のデータは当然暗号化され、且つスクランブルされたデータとして保存される。

【００６５】また、この時生成した秘密値Nraは、図９に示すように秘密メモリ５内に確保されたパスワードＰｗ３に対応してこれに保存され（ステップ８１）、このパスワードＰｗ３によって照合などの操作が可能とされる。そして、ステップ８２でスクランブル符号発生器６の出力と、暗号処理器７の暗号化／復号化機能と停止してこのフローを終了する。

【００６６】以上のステップによって所望のアプリケーションソフトDexeXが暗号化された状態でハードディスク２２にインストールされ、更に必要な諸環境が初期設定されたことになる。

【００６７】次に、所望のアプリケーションソフトを実行する場合の手順について、図５，６の実行フローチャートを参照しながら説明する。説明を容易にするため、ここで実行するアプリケーションソフトを、上記の説明でインストールされたDexeXとする。

【００６８】ステップ４１でこのアプリケーションソフトが実行されると、このソフトの読み込みが行なわれる（ステップ４２）。このステップ４２の行程は、前記した図２の示すフローチャートのステップ２からステップ１０の行程に対応するもので、既に説明したように暗号化スクランブルされたアプリケーションソフトEsf３（DexeX(+)Ｆ(ReX)）がメインメモリ２１にロードされると共に、パーミットコードEpmp（Ksf３）が復号され、作業鍵Ksf３が保管レジスタ８に保管される。

【００６９】更に、スクランブル符号発生器６の出力を開始し、暗号処理器７の暗号化／復号化機能を起動するための指令信号ｓ１を出力する。これにより、後述するステップ４９で両機能がオフとされるまで、CMP１とメインメモリ２１等の外部記憶装置との間で入出力するデータはすべて暗号化されたものとなる。

【００７０】尚、図２で説明したように、この暗号化スクランブルされたアプリケーションソフトEsf３（DexeX(+)Ｆ(ReX)）には前記した起動処理プログラムが添付されているものとする。また今回は、図４のフローに基づくインストール時にパーミットコードの保管が行なわれるので、結果的に図２中の起動処理プログラムによるステップ４からステップ６の行程を省略できる。

【００７１】そして、このソフトの環境設定ファイルAcfg３を読み出し、この中にパスワードＰｗがあるか確認する（ステップ４３）。このケースでは、パスワードＰｗ３が存在するのでステップ４４に至るが、もし存在しない場合、このソフトのインストール時にエラーが生じてパスワードが生成されなかったことを意味するので、このことを図示しない表示手段で表示して再インストールの指令を出し（ステップ４５，４６）、更にステップ４９でスクランブル符号発生器６の出力と暗号処理器７の機能とを停止した後、待機状態に戻る。

【００７２】次にステップ４４でこのアプリケーションソフトの時間データファイルDdat（Ddat＝Tre＋Nra）が読み出される。この時、当然作業鍵Ksf３による復号化とアドレスによるデスクランブルが行なわれる。尚、この時読み出される暗号化された時間データファイルDdatは、必要に応じてメインメモリ２１にそのままの形で保管される。

【００７３】次に、秘密メモリ５内の秘密値Nraと時間データファイルDdatの秘密値との照合が行なわれる（ステップ４７）。今は、上記図４のインストールフローの説明でインストールされたアプリケーションソフトDexeXの秘密値が照合されるため、この時間データファイルDdatが何らかの方法で改ざんされないかぎりこ

れら２つの秘密値は一致し、ステップ５０に移行することが理解される。

【００７４】もしここで、前記したような時間データファイルDdatの置き換えが行なわれていると、当然これら２つの秘密値が異なるためステップ４８に移行し、後述する処理が行なわれる。

【００７５】ステップ５０乃至ステップ５３は、アプリケーションソフトDexeXを実行処理すると同時に残量時間を監視するフローになっている。即ち、ステップ５０では実行時間を計測して逐次残量時間を更新し、ステップ５１では残量時間がゼロになったかを監視し、更にステップ５３ではこの実行の停止指令が入ったかどうかを監視する。

【００７６】また、このステップ５２では、必要に応じて順次メインメモリ２１にロードされたアプリケーションソフトEsf３（DexeX(+)F(ReX)）がＣＰＵ２へ読み込まれるが、その際には前記した復号化、及びデスクランブルが逐次実行される。

【００７７】この実行中に残量時間がゼロになるとステップ５１でこれを判定し、一旦ソフト処理を終了した後（ステップ５４）、図示しない表示手段によって例えば「残量時間がありません。」等の表示を行なって（ステップ５５）、後述するようにソフト供給元に残量時間の追加を申請するプログラムに入る（ステップ５６）。今は、インストールされたばかりのアプリケーションソフトDexeXの例を想定して記述しているので残量時間がゼロになっており、当然このルートをたどる。

【００７８】このステップ５６の残量時間追加申請プログラムは、図７に示すフローチャートに示す手順によって行なわれる。即ちユーザーは、残量時間がなくなって暗号化された状態の時間データファイルDdatを何等かの方法でソフト供給元に届ける（ステップ９１）。その方法は種々考えられるが、例えばモデム２５を介して行なわれるインターネットなどのパソコン通信によって行なってもよい。

【００７９】一方、ソフト供給元では、このファイルの復号化とデスクランブルを行なってデータを復元し、このDdat（Ddat＝Tre＋Nra）の残量時間Treの追加補充を行なう（ステップ９２）。その補充量は、ユーザーの依頼に応じて決定されるが、対価の補充料金の支払については別途行なわれるものとし、ここでの説明は省略する。

【００８０】ソフト供給元では、この残量時間Treの補充を行なった後、一緒に送られてきた秘密値と共に、再びアドレススクランブルと作業鍵Ksf３による暗号化を行なった後ユーザーに返信する（ステップ９３）。この方法も、パソコン通信を介して行なってもよいし、フロッピィディスクに納めて郵送するようにしてもよい。

【００８１】ユーザーは、この時間補充された時間データファイルを再度入手し、前のデータファイルと置き換える如くこれをハードディスク２２に保存し（ステップ９４）、この残量時間追加申請のフローを終了する。従って、この時のDdat（Ddat＝Tre＋Nra）において、残量時間Treは所定量補充されているものの、秘密値Nraは、秘密メモリ５に保存されている秘密値と同じままであることが理解される。

【００８２】ユーザーは、このアプリケーションソフトDexeXを引き続いて実行したい場合、再度図５の実行フローのステップ４１に戻らなければならない。然し乍ら今回は、残量時間が所定量補充されているので、ステップ４１で実行が指令されると、ステップ５０乃至ステップ５３のフローが繰り返されて、アプリケーションソフトDexeXの実行状態が継続されることになる。

【００８３】そして、残量時間Treがゼロとなる前に、ユーザーによるソフト処理終了の指令を受けると、次のステップ５７に至る。このステップ５７では、乱数を発生して秘密値Nra'を更新し、その後この更新した秘密値Nra'とこの時のソフトの実行時間が差し引かれた残量時間Treとを対にして新たな時間データファイルDdat（Ddat＝Tre＋Nra'）を作成する（ステップ５８）。尚、この時作成されたデータDdatは、必要に応じて一旦メインメモリ２１に保存されるが、この際のデータは当然暗号化され、スクランブルされたデータとして保存される。

【００８４】そしてこれをハードディスク２２に保存されている更新前の時間データファイルに代えて保存する（ステップ５９）と共に、更新された秘密値Nra'を、秘密メモリ５内に確保されたパスワードＰｗ３によって識別可能に同メモリ内に保持されている更新前の秘密値に代えて保存する（ステップ６０）。

【００８５】この時、前記した更新前の秘密値Nraの照合が行なわれる。図１１に示すフローチャートは、ステップ６０内で行なわれるこの照合動作の流れを示すもので、ステップ６０－１では秘密メモリ５内の秘密値Nraと照合のために別途用意されたNraとが合致するかをチェックする。これ等が合致する場合はステップ６０－２で上記したデータの更新が行なわれ、合致しない場合は、ステップ６０－３に至って、図示しない表示手段によって、「不正が行なわれました。」等の表示を行ない、図５のＢへ戻るように構成しても良い。

【００８６】そして再度このアプリケーションソフトDexe３が実行されると、上記した各ステップを経てステップ４７に至り、ここで秘密値が照合される。この時、秘密メモリから読み出した秘密値とハードディスク２２から読み出された秘密値とは一致するはずであるが、もし、ユーザーによって前記したようなデータの改ざんがあるとこれ等は一致しない。この時はステップ４８に至って「不正行為が行なわれました。」等のメッセージを表示し、実行を中止すべくステップ４９を経由して待機状態に戻る。

【００８７】一方、このアプリケーションソフトDexeXの使用を中止し、アンインストールする場合には、このソフトに設定されたパスワードＰｗ３と秘密値Nraを秘密メモリ５から消去する必要がある。これを行なわないと同メモリ内に不要な秘密値が蓄積されることになる。またこの消去作業はアンインストール時のみに、またハードディスク２２にパスワードが存在する段階で行なわれる必要があるため、例えば、図８に示すフローに従って行なわれる。

【００８８】即ち、図示しない入力手段によってアンインストールの指示を受けると、ステップ１０１に至り、先ずパスワードと秘密値の消去が行なわれる。この際にも、安全性を高めるために前記したような秘密値Nraによる照合が行なわれる。このために(Ｐｗ３，Nra)が用意され、パスワードＰｗ３によって識別された秘密メモリ５内のNraと照合のために用意したNraとが一致した場合にのみこのアプリケーションソフトDexeXに対応するパスワードＰｗ３と秘密値Nraとが同時に消去される。そしてこの消去が終了した後、アプリケーションソフトDexeX自体のアンインストールが実行される（ステップ１０２）。

【００８９】次に、本発明の他の実施例について説明する。図１４は、秘密メモリ部５１がＣＭＰ５０の外にあって独立して存在する場合を示し、その他の前記した図１と同じ機能を有する構成要素については、同符号を付してその説明を省略する。図１に対する図１４の構成上の違いは、ＣＭＰ１内部にあった秘密メモリがその外部の秘密メモリ部５１に照合手段５２と共に独立して設けられた点であり、全体的な機能は全く同じである。

【００９０】一方、図１に対する図１４の部分的な機能の相違点は、図１の構成では秘密メモリ５の内部データがＣＭＰ１の外部に出力されないように構成されているのに対し、図１４の構成では秘密メモリ部５１の内部データがその外部に出力されないように構成される点である。

【００９１】従って、図１のＣＭＰ１内に設けられた秘密メモリの働きについて、図４乃至図７のフローチャートを参照して説明したが、図１４構成のＣＭＰ５０外に設けられた秘密メモリ部５１についても、これ等のフローチャートに従って同様の作業が実行できる。しかしながら、図５のステップ４７、図１１のステップ６１－１、及び図８のステップ１０１の各ステップで行なわれる照合作業は、秘密メモリ部５１内部の照合手段５２で行なわれ、YES,NOの結果のみが出力されるように構成されている。

【００９２】次に、本発明の他の実施例について説明する。図１２は、本発明の他の実施例を示す構成図で、前記した図１と同じ機能を有する構成要素については、同符号を付してその説明を省略し、図１の構成及び動作と異なる部分について重点的に説明する。

【００９３】この実施例の場合、暗号化されアドレススクランブルされたデータＤを前記した標記方法に従って標記すると、Escri（D）となる(i=1, 2, 3……N)。但しこの秘密鍵Kscriは、Kscri＝Ksf(+)Ｆ(Rei)ということになる。即ち、このデータＤに用意される作業鍵Ksfと逐次生成されるスクランブル符号Ｆ(Rei)との排他論理和符号によってデータＤを暗号化したものとなる。

【００９４】このようにして暗号化されたアプリケーションソフトを図１２のＣＭＰによって復号化する過程を説明する。いま、このアプリケーションソフトの１バイト単位のデータ群D1，D2……DNの集合をＤＸと記述し、これに対応して生成されるスクランブル符号群Ｆ（Re1），Ｆ（Re2)……Ｆ（ReN)の集合をＦ（ReX)と記述し、この暗号化されたアプリケーションソフトをＥｓｃｒ（ＤＸ）と記述する。但し、Kscr＝Ksf(+)Ｆ(ReX)である。

【００９５】従って、いま最初の１バイトのデータD1を復号する過程を記述すると、この時データバス１２には、暗号化されたデータEscr1（D1）が現れ、スクランブル符号発生器６からはＦ(Re1)が出力される。従ってこの時の暗号処理器７は、作業鍵Ksfとスクランブル符号Ｆ(Re1)の排他論理和符号Ksf(+)Ｆ(Re1)によってデータEscr1（D1）を復号することになるため、暗号化した時と同じ鍵でこれを復号化して得たデータD1をＣＰＵ２に出力することが出来る。以下同様にして、全ての暗号化されたデータ群を順次復号化してＣＰＵ２に送る。

【００９６】先に、図１に示す構成のＣＭＰ１による、アプリケーションソフトの入手、及びその実行に際してのＣＰＵ２内への読み込み過程について、図２のフローチャートを参照しながら説明したが、図１２構成のＣＭＰ３０もこのフローチャートに従って同様の作業が実行できる。但し、ステップ１１の復号方法が上記した説明に基づいて実行されるところが異なる。

【００９７】また、ユーザーによって作成され、一旦メインメモリ２１に保存したデータを、図１の構成のＣＭＰによって暗号化して再度メインメモリに保存しなおす過程を図３のフローチャートを参照して説明したが、図１２構成のＣＭＰ３０もこのフローチャートに従って同様の作業が実行できる。但し、ステップ２８の暗号化方法が異なり、排他論理和符号（Kusr(+)Ｆ(ReX)）によってデータ群ＤＸを逐次暗号化するものとなる。

【００９８】更に、図１の構成のＣＭＰ１内に設けられた秘密メモリの働きについて、図４乃至図７のフローチャートを参照して説明したが、図１２構成のＣＭＰ３０内に設けられた秘密メモリ５についても、これ等のフローチャートに従って同様の作業が実行できる。但し、フローで実行されるデータの暗号化又は復号化の方法が図１のＣＭＰ１と異り、上記したように排他論理和符号（Kusr(+)Ｆ(ReX)）を作業鍵として行なわれる。

【００９９】次に、本発明の他の実施例について説明する。図１３は、本発明の他の実施例を示す構成図で、前記した図１と同じ機能を有する構成要素については、同符号を付してその説明を省略し、図１の構成及び動作と異なる部分について重点的に説明する。

【０１００】この実施例の場合、暗号化されアドレススクランブルされたデータＤを前記した標記方法に従って標記すると、Ｅsss（Ｄ(+)Ｆ(Re)）となる。但しこの作業鍵Ksssは、Ksss＝Ｅssp(Kusr)ということになる。即ち暗号部４１は、ＣＰＵ２からユーザーによって設定される作業鍵Kusrを入力し、保管レジスタ１０が保管しているこのＣＭＰ４０に固有の秘密鍵Ksspでこれを暗号化した前記作業鍵Ksssを生成し、これを保管レジスタ８に出力する。

【０１０１】暗号処理部７は、この保管レジスタ８に保管された作業鍵Ksssでアドレススクランブルされたデータ（Ｄ(+)Ｆ(Re)）を暗号化し、この暗号化したデータＥsss（Ｄ(+)Ｆ(Re)）をデータバス１２を介してメインメモリ２１等の外部メモリに出力する。

【０１０２】このようにして暗号化されたデータを図１３のＣＭＰによって復号化する過程を説明する。いま、データの１バイト単位のデータ群Ｄ1，Ｄ2……ＤＮの集合をＤＸと記述し、これに対応して生成されるスクランブル符号群Ｆ（Re1），Ｆ（Re2)……Ｆ（ReN)の集合をＦ（ReX)と記述し、このスクランブル暗号化されたデータをＥsss（ＤＸ(+)Ｆ(ReX)）と記述する。但し、Ksss＝Ｅssp(Kusr)である。

【０１０３】従って、いま最初の１バイトのデータＤ1を復号する過程を記述すると、この時データバス１２には、暗号化されたデータＥsss（Ｄ1(+)Ｆ(Re1)）が現れ、スクランブル符号発生器６からはＦ(Re1)が出力される。従って暗号処理器７は、この時作業鍵Ksssでデータ Ｅsss（Ｄ1(+)Ｆ(Re1)）を復号化した（Ｄ1(+)Ｆ(Re1)）を加算器１１に出力し、加算器１１はＦ(Re1)でこれをデスクランブルして得たデータＤ1をＣＰＵ２に出力することが出来る。以下同様にして、全ての暗号化されたデータ群を順次復号化してＣＰＵ２に送る。

【０１０４】また、ユーザーによって作成され、一旦メインメモリ２１に保存したデータを、図１の構成のＣＭＰによって暗号化して再度メインメモリに保存しなおす過程を図３のフローチャートを参照して説明したが、図１３構成のＣＭＰもこのフローチャートに従って同様の作業が実行できる。但し、ステップ２３では作業鍵Ksss＝Ｅssp(Kusr)を保管レジスタ８に保管する必要があり、このため前記した暗号部４１よる作業鍵Kusrの暗号化が行なわれる。

【０１０５】従って、この図１３に構成されたＣＭＰ４０によって暗号化されたデータは、この暗号化したＣＭＰのみによって復号化されることが理解される。更に、作業鍵Ksssが二重鍵の構成を有するため、暗号化するデータ群ごとに作業鍵を変えることができるために鍵自体が解読されにくくなり、データの氾濫を防ぐと共にその機密性を高めることが出来る。

【０１０６】次に、本発明の他の実施例について説明する。図１５は、本発明の他の実施例を示す構成図で、前記した図１と同じ機能を有する構成要素については、同符号を付してその説明を省略し、図１の構成及び動作と異なる部分について重点的に説明する。

【０１０７】この実施例の場合、作業鍵の保管レジスタ８を複数Ｐ個有する保管レジスタ部６１を設け、これ等の各保管レジスタに異なる作業鍵Ksfi(i=1, 2, ……P)をそれぞれ保管可能とする。この保管レジスタ部６１は、復号部９から出力される作業鍵を保管するレジスタの選択、及び暗号処理部７に出力する作業鍵の選択を、制御ユニット３から出力される鍵選択信号ｓ５によって実行できるように構成されている。

【０１０８】また、オフセットレジスタ部６２には、前記したデータ群の先頭アドレスを保管するための複数Ｐ個のオフセットレジスタ４が、異なる先頭アドレスToi(i=1, 2, ……P)をそれぞれ保管可能に設けられ、制御ユニット３から出力される先頭アドレス選択信号ｓ６によって、先頭アドレスToiの保存、及び読み出しの対象となるレジスタが選択可能に構成されている。

【０１０９】次にこのような構成のＣＭＰ６０の動作について説明する。今、前記した図２の実行準備フローが実行され、そのステップ３の段階でメインメモリ２１にロードされたソフトが図１７に示すようにＭ個のプログラムから構成され、それぞれが異なる作業鍵Ksfj（j=1, 2, ……M、M≦Ｐ）で暗号化されているものとする。

【０１１０】また各プログラムは、前記したようにそれぞれ所定単位のデータの集合であるデータ群で構成され、各データ群の先頭アドレスをToj（j=1, 2, ……M）と記す。　この場合の各作業鍵Ksfjは、各プログラムを管理するソフト供給元が前記したパーミットコードとして供給するため、図２の実行準備フローのステップ４からステップ９までのステップが図１のＣＭＰ１と異なる。

【０１１１】即ち、ステップ４からステップ６までで、パーミットコードの存在の確認、入手、保存の各行程を実施するが、今このパーミットコードがＭ個必要となるため、この各行程もＭ回繰り返すように構成される。更に、ステップ７からステップ９までの行程で、パーミットコードを読み込み、それを復号し、生成した作業鍵をレジスタに保存するが、ここでもこの各行程をＭ回繰り返すように構成される。

【０１１２】この時逐次生成される作業鍵Ksfjが、ＣＰＵから出力される指令信号ｓ１に基づいて制御ユニット３から出力される鍵選択信号ｓ５によって選択された１からＭまでの各保管レジスタ８にそれぞれ保管される。

19

【０１１３】更にステップ１１で、必要に応じてメインメモリ２１に保管された各プログラムがＣＰＵ２に読み込まれて実行される際には、それぞれのプログラムの作業鍵Ksfjを保管するレジスタが選択され読み出され、暗号処理器７に供給される。これと共に、読み出されるプログラムに対応する先頭アドレスがＣＰＵから出力される指令信号ｓ１に基づいて制御ユニット３から出力されるアドレス選択信号ｓ６によって選択される。そして選択された先頭アドレスTojがスクランブル符号発生器６に出力され、前記したアドレススクランブルが各プログラム毎に実行される。尚、ｉとｊとが対応して管理されることにより、各プログラムとこれを実行する際に読み出される各作業鍵、及び各先頭アドレスとの対応関係が維持される。

【０１１４】次に、本発明の他の実施例について説明する。図１６は、本発明の他の実施例を示す構成図で、前記した図１と同じ機能を有する構成要素については、同符号を付してその説明を省略し、図１の構成及び動作と異なる部分について重点的に説明する。

【０１１５】この実施例の場合、復号部７２と保管レジスタ７３とからなる多重鍵生成部７１が追加構成される。そして保管レジスタ７３は、このＣＭＰ７０に固有の秘密鍵Ksmppを保管し、復号部７２は前記した公開鍵Kpmpに対応する秘密鍵Ksmpを、秘密鍵Ksmppに対応する公開鍵Kpmppで暗号化したEpmpp（Ksmp）を得て秘密鍵Ksmppで復号化し、生成した秘密鍵Ksmpを保管レジスタ１０に出力する。

【０１１６】このように構成することにより、ＣＭＰ７０にとって、一対の公開鍵Kpmpと秘密鍵Ksmpとがすでに登録された固有のものではなく、例えばＣＭＰ７０の供給元から別途これ等の鍵を入手して設定することが出来るなど、種々の態様を可能とするものとなる。

【０１１７】

【発明の効果】本発明によれば、ソフト供給元は、供給するソフトを所定のＣＭＰでのみ利用させることが可能となるだけでなく、同一のアプリケーションソフトは同じ鍵で暗号化されるため、暗号化したアプリケーションソフトをＣＤ－ＲＯＭ等の複製のみ可能な媒体によって市場に出すことができる。一方、図１３の構成の本発明によれば、ＣＭＰ固有の秘密鍵で暗号化された作業鍵によってデータ群を暗号化／復号化するため、同じＣＭＰでしか解読出来ないデータとなり、データの漏洩による不利益を防ぐことが出来る。

【図面の簡単な説明】

【図１】本発明の一実施例を示す構成図

【図２】本発明の動作説明に供するフローチャート

20

【図３】本発明の動作説明に供するフローチャート

【図４】本発明の動作説明に供するフローチャート

【図５】本発明の動作説明に供するフローチャート

【図６】本発明の動作説明に供するフローチャート

【図７】本発明の動作説明に供するフローチャート

【図８】本発明の動作説明に供するフローチャート

【図９】本発明の動作説明に供する秘密メモリの説明図

【図１０】本発明の動作説明に供するアプリケーションソフトの構成図

【図１１】本発明の動作説明に供するフローチャート

【図１２】本発明の他の一実施例を示す構成図

【図１３】本発明の他の一実施例を示す構成図

【図１４】本発明の他の一実施例を示す構成図

【図１５】本発明の他の一実施例を示す構成図

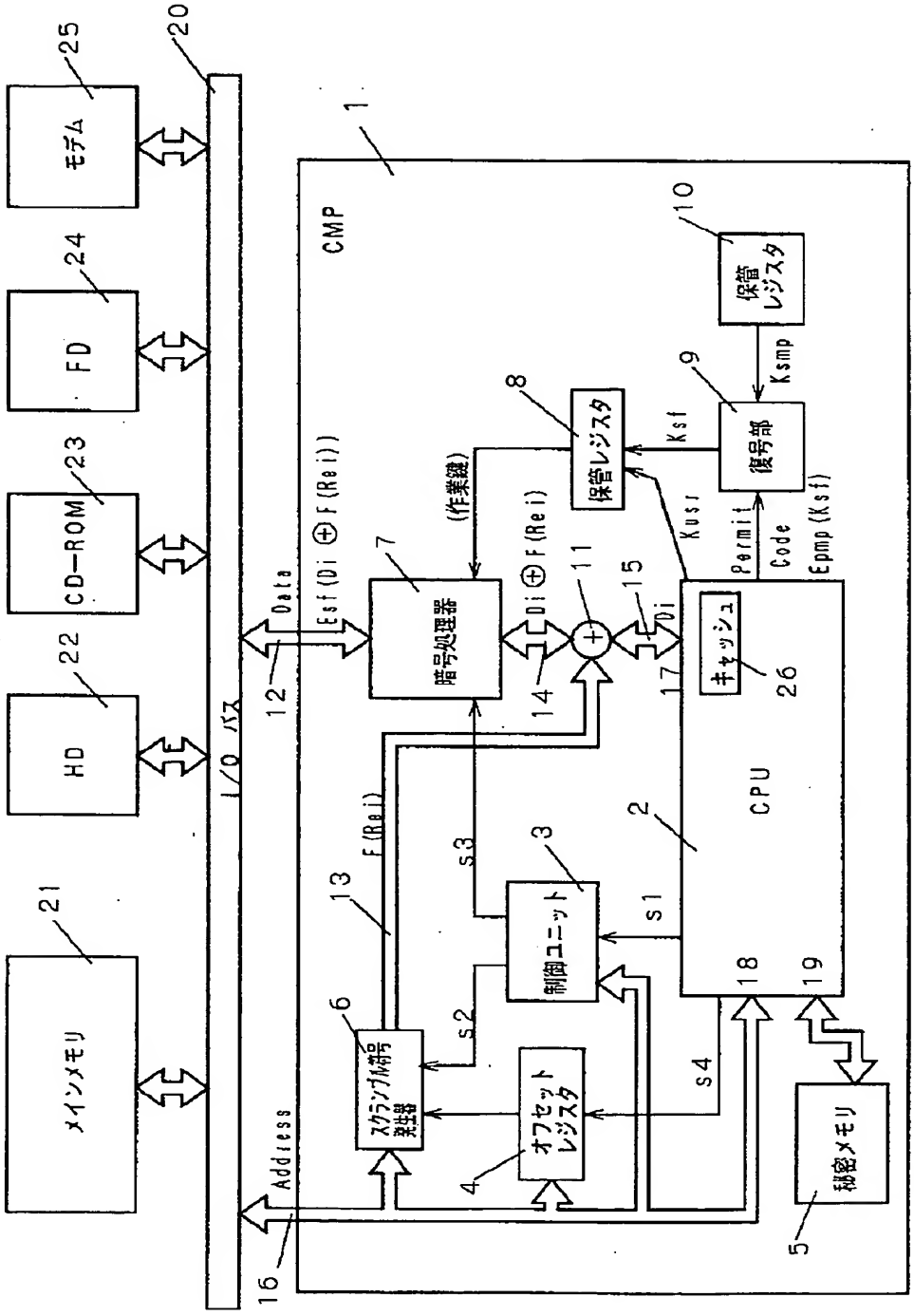
【図１６】本発明の他の一実施例を示す構成図

【図１７】本発明の動作説明に供するメインメモリの説明図

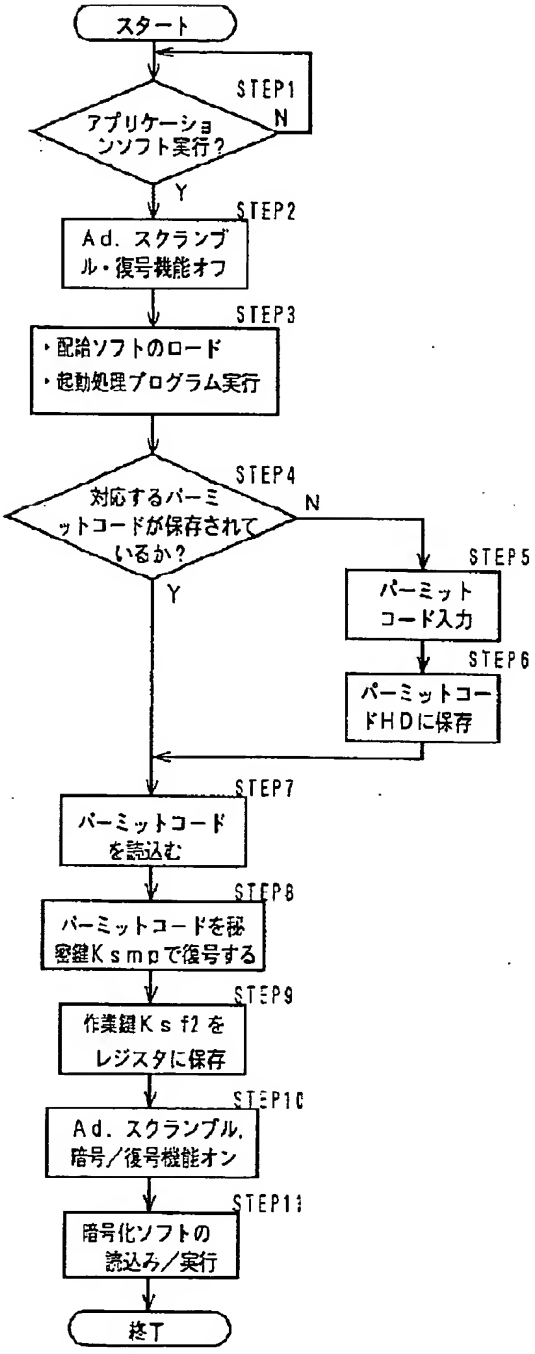
【符号の説明】

１　ＣＭＰ
２　ＣＰＵ
３　制御ユニット
４　オフセットレジスタ
５　秘密メモリ
６　スクランブル符号発生器
７　暗号処理器
８　保管レジスタ
９　復号部
１０　保管レジスタ
１１　加算器
２１　メインメモリ
２２　ハードディスク
２３　ＣＤ－ＲＯＭ
２４　フロッピディスク
２５　モデム
２６　キャッシュメモリ
３０　ＣＭＰ
４０　ＣＭＰ
４１　暗号部
５０　ＣＭＰ
５１　秘密メモリ部
５２　照合手段
６０　ＣＭＰ
６１　保管レジスタ部
７０　ＣＭＰ
７１　多重鍵生成部

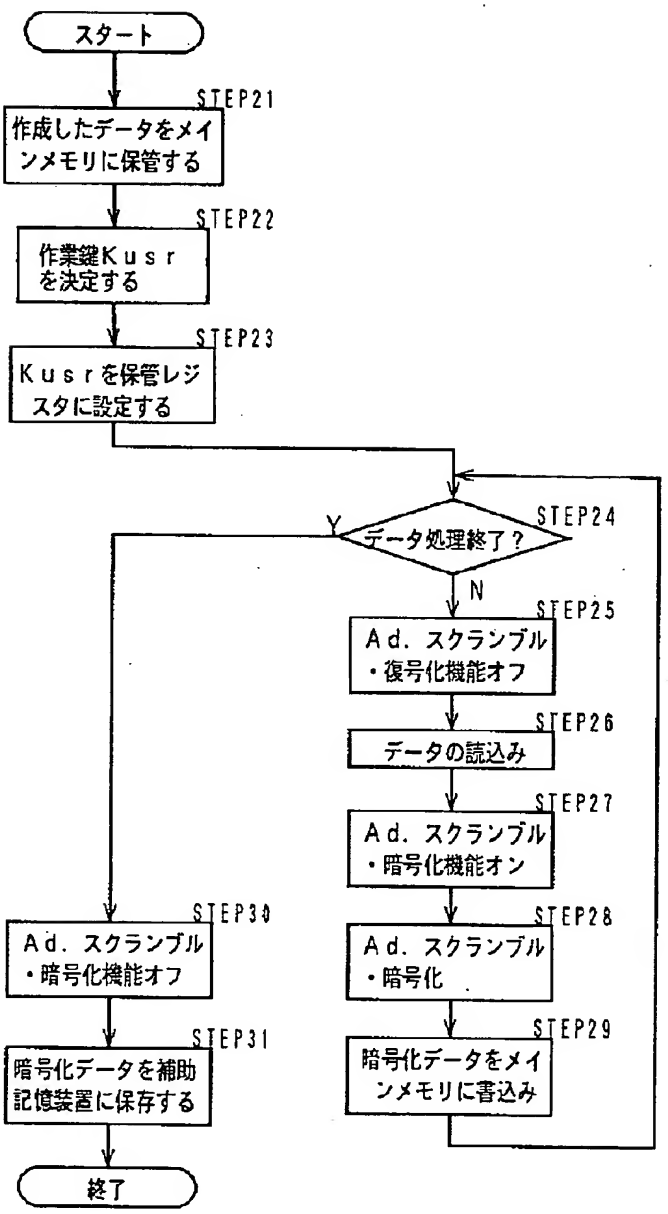
【図１】


CMP
CPU
I/O バス
モデム
FD
CD-ROM
HD
メインメモリ
暗号処理器
制御ユニット
スクランブル符号発生器
オフセットレジスタ
保管レジスタ
復号部
キャッシュ
秘密メモリ
(作業鍵)
Esf(Di ⊕ F(Rei))
Di ⊕ F(Rei)
F(Rei)
Data
Address
Di
Kusr
Ksf
Ksmp
Permit
Code
Epmp(Ksf)
s1
s2
s3
s4

【図２】



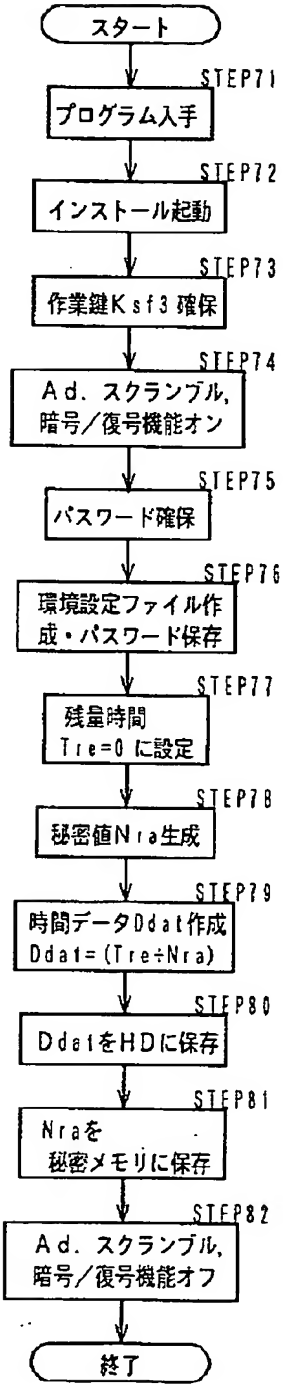

【図３】



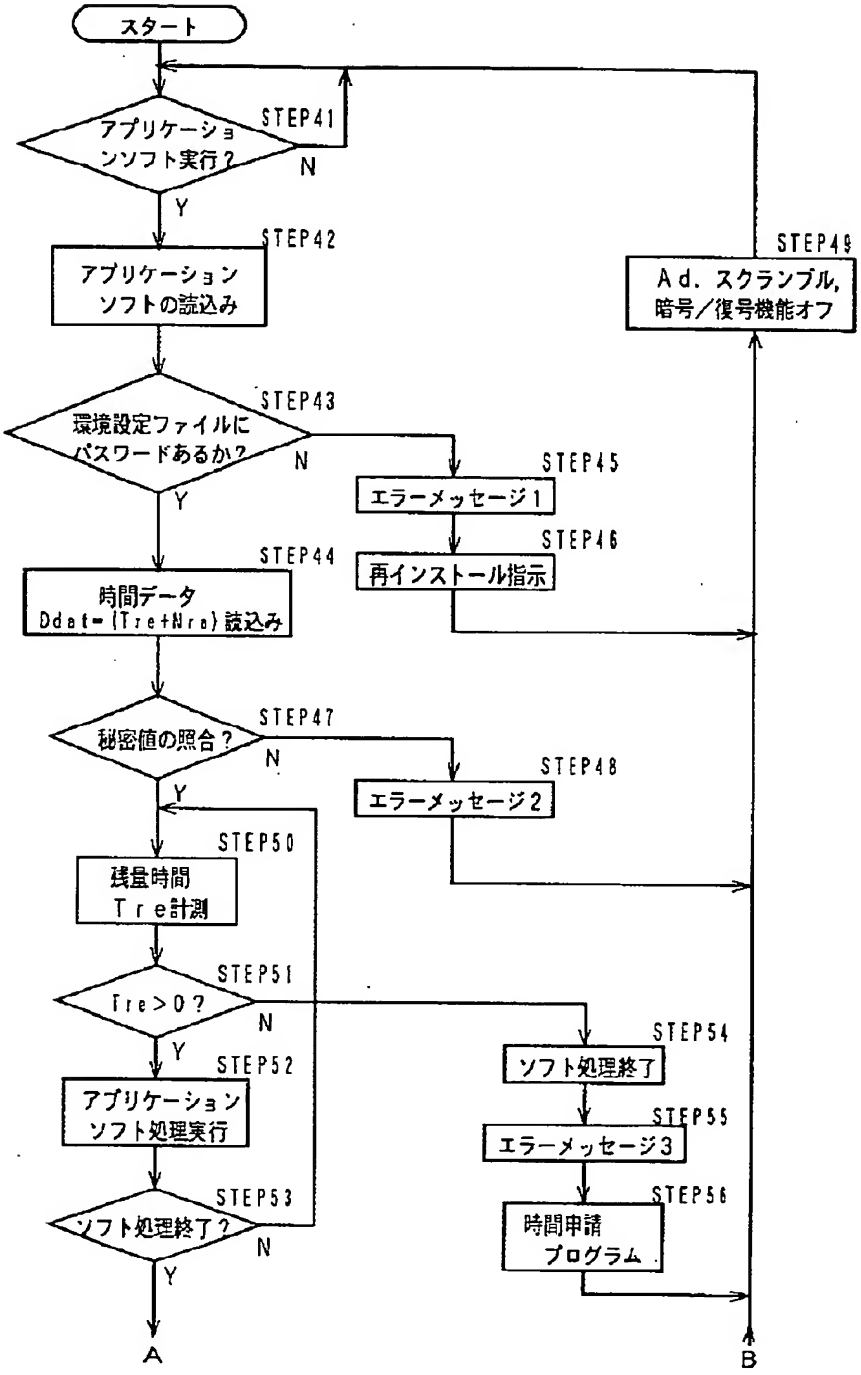

【図１０】

| | |
|---|---|
| 起動処理プログラム | 暗号化アプリケーションソフト<br>Esf2(DapX⊕F(ReX)) |

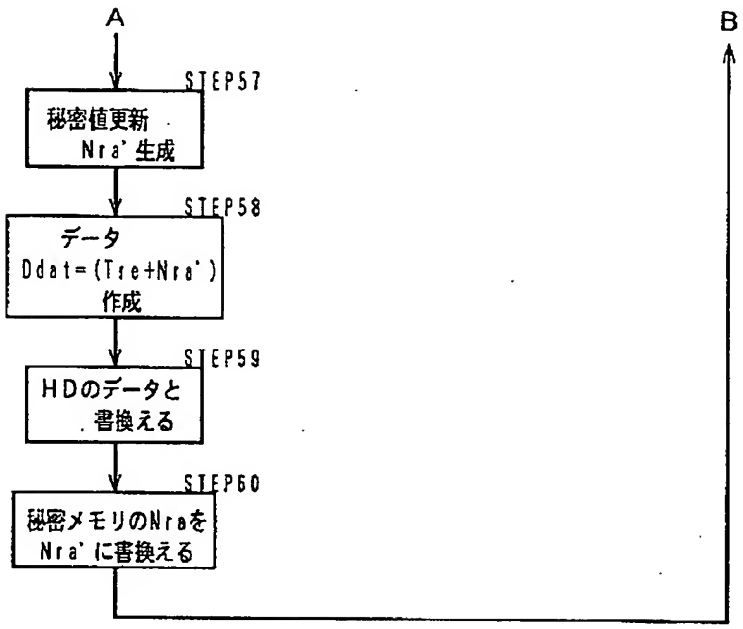
【図４】


スタート
STEP71
プログラム入手
STEP72
インストール起動
STEP73
作業鍵Ksf3確保
STEP74
Ad．スクランブル，暗号／復号機能オン
STEP75
パスワード確保
STEP76
環境設定ファイル作成・パスワード保存
STEP77
残量時間 Tre=0 に設定
STEP78
秘密値Nra生成
STEP79
時間データDdat作成 Ddat=(Tre÷Nra)
STEP80
DdatをHDに保存
STEP81
Nraを 秘密メモリに保存
STEP82
Ad．スクランブル，暗号／復号機能オフ
終了

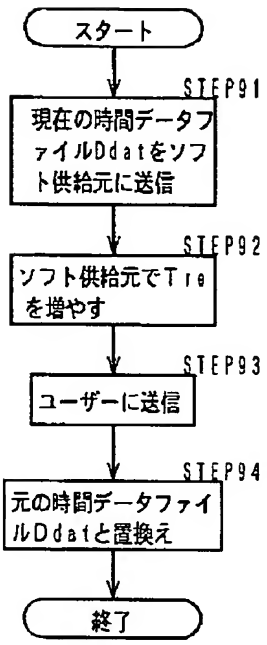
【図５】


スタート
STEP41
アプリケーションソフト実行？
N
Y
STEP42
アプリケーション ソフトの読込み
STEP43
環境設定ファイルにパスワードあるか？
N
Y
STEP45
エラーメッセージ1
STEP46
再インストール指示
STEP44
時間データ Ddat=(Tre+Nra) 読込み
STEP47
秘密値の照合？
N
Y
STEP48
エラーメッセージ2
STEP50
残量時間 Tre計測
STEP51
Tre>0？
N
Y
STEP52
アプリケーション ソフト処理実行
STEP53
ソフト処理終了？
N
Y
A
STEP54
ソフト処理終了
STEP55
エラーメッセージ3
STEP56
時間申請 プログラム
STEP49
Ad．スクランブル，暗号／復号機能オフ
B

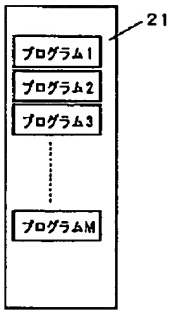
【図６】



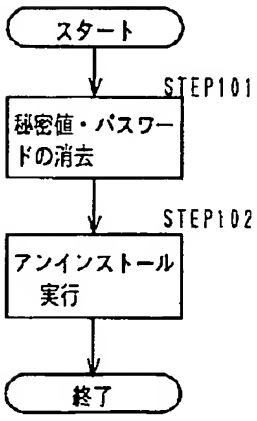

【図７】




【図１７】



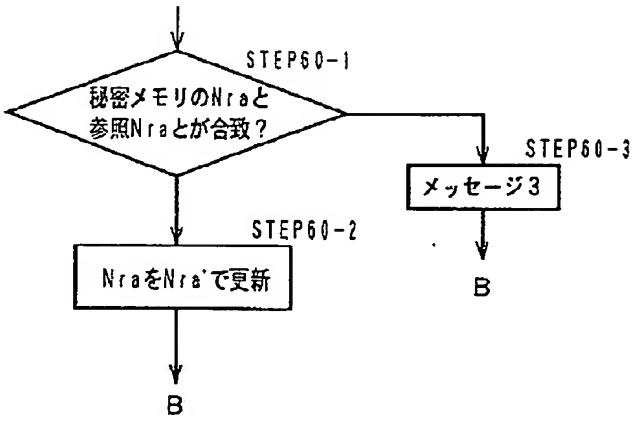

【図８】



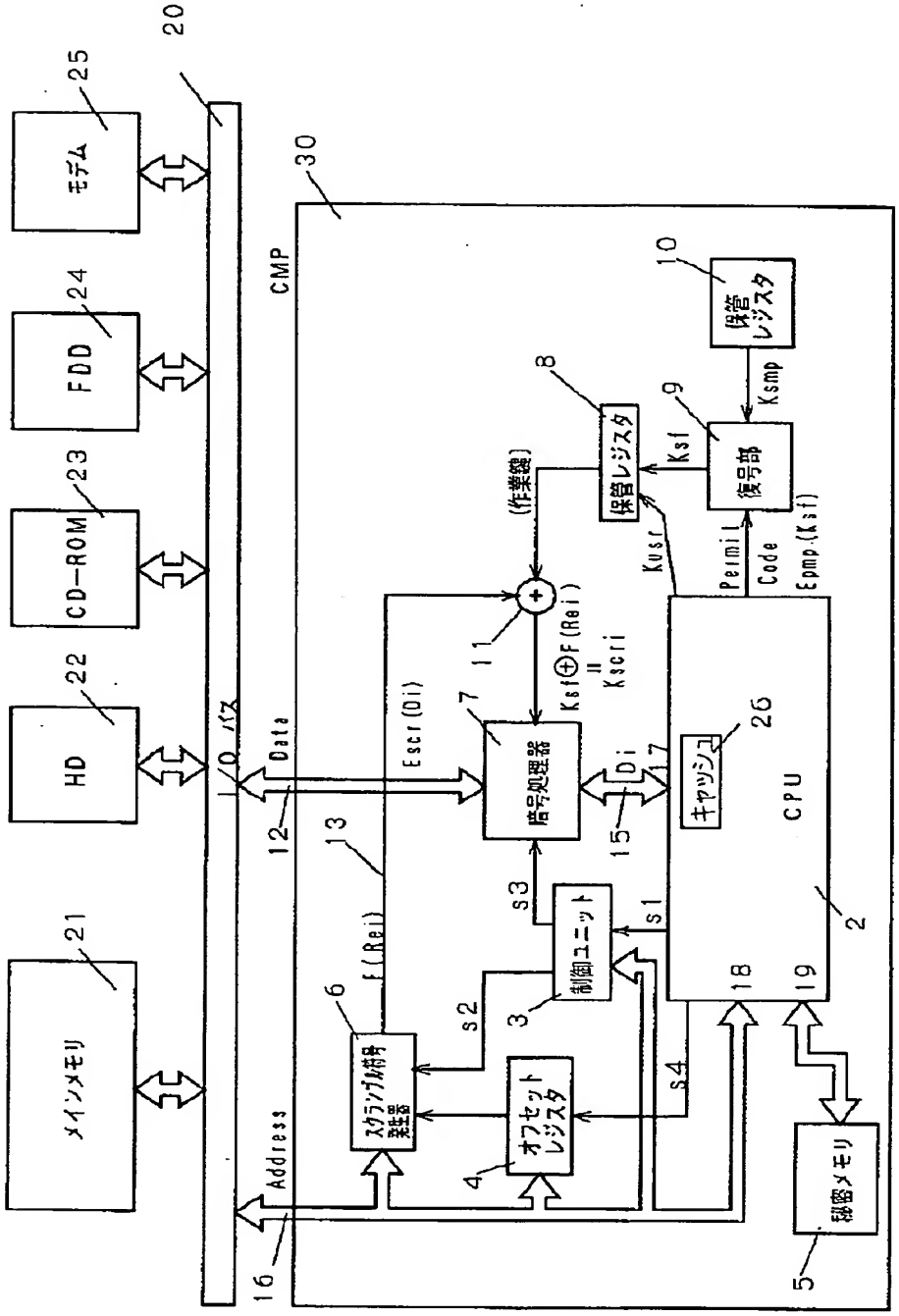

【図９】

| パスワード | 秘密値 |
|---|---|
| PW1 | Nra1 |
| PW2 | Nra2 |
| PW3 | Nra3 |
| ｜ | ｜ |
| PW n | Nra n |

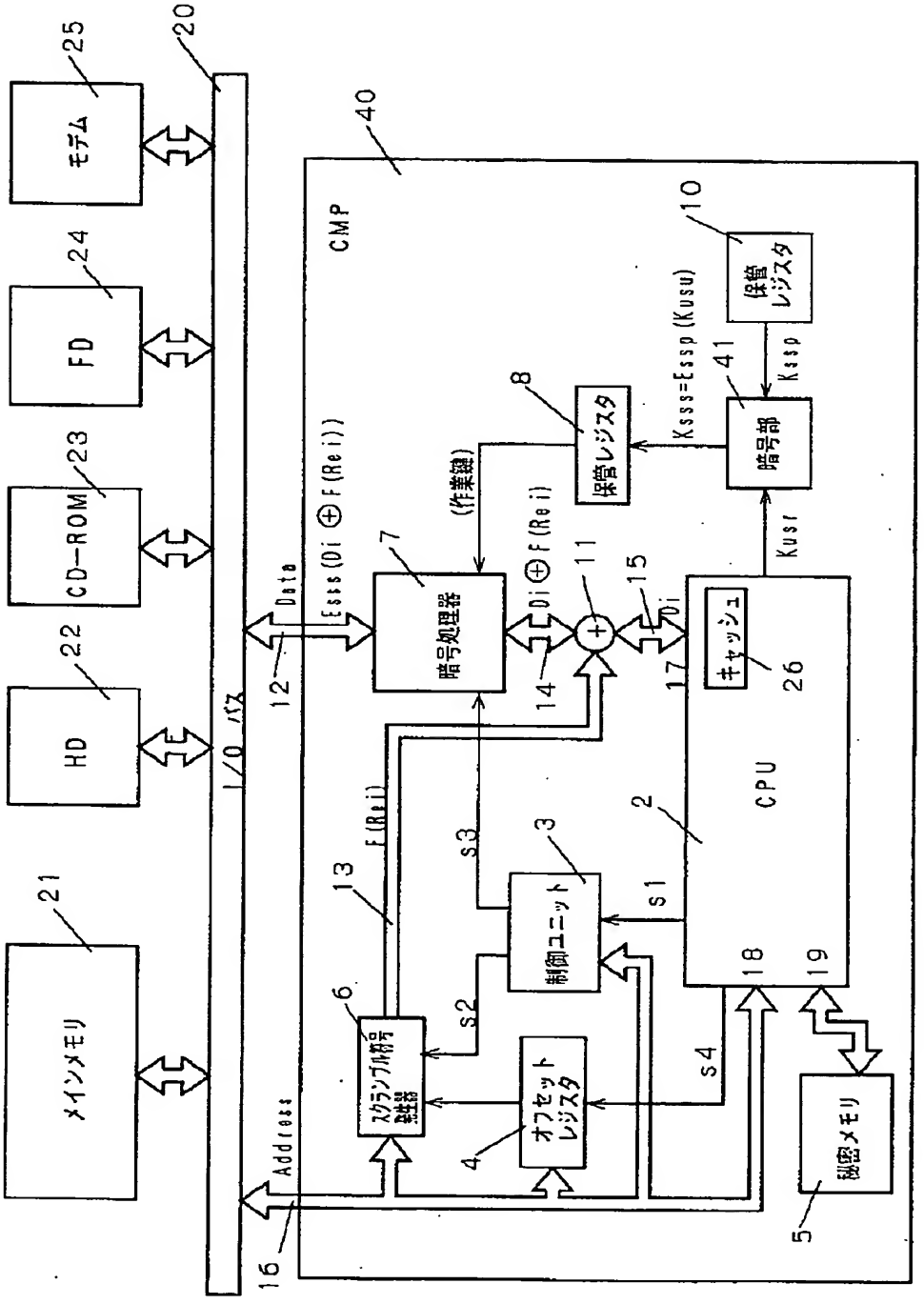
【図１１】



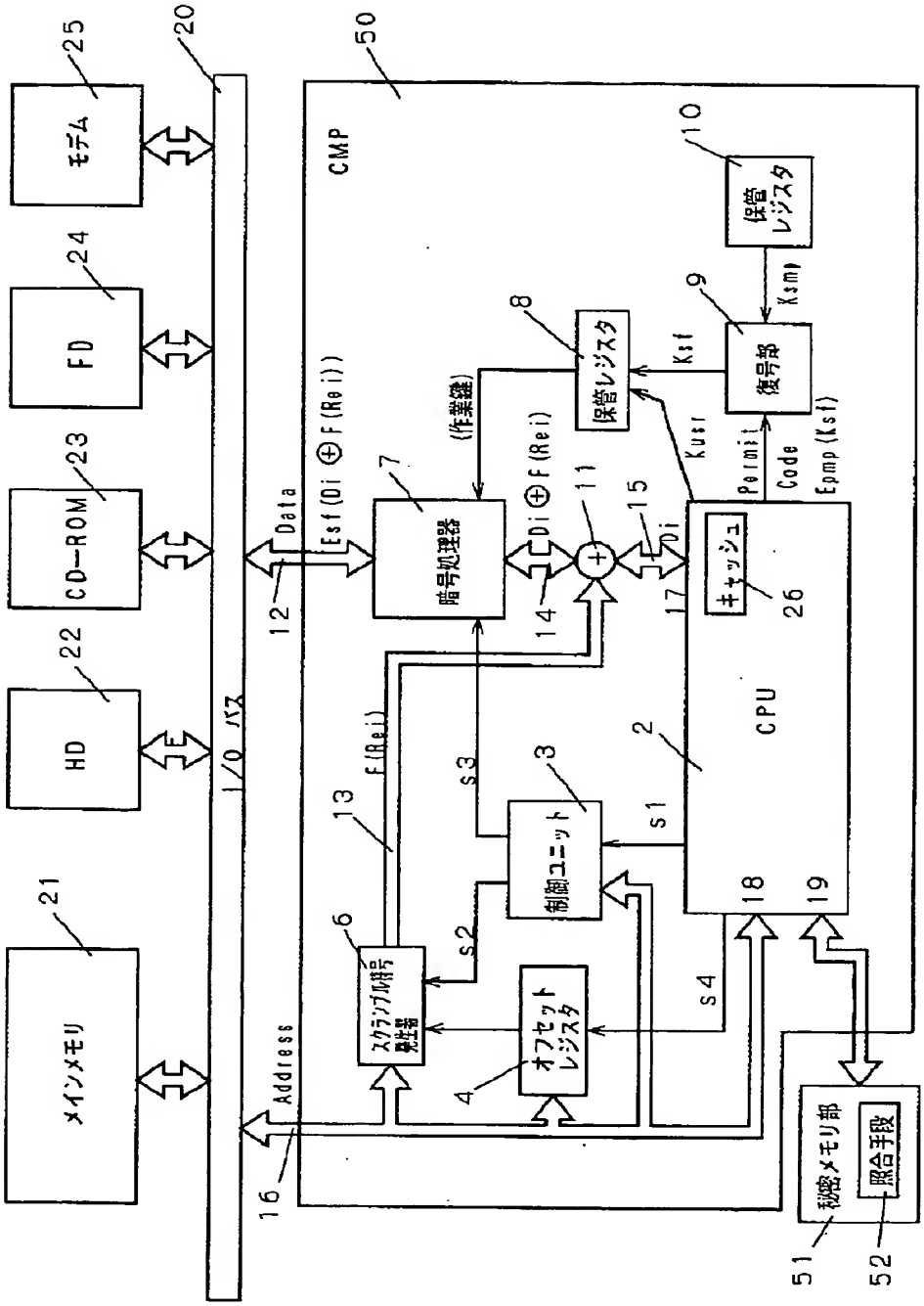
【図１２】


20
25
モデム
24
FDD
23
CD-ROM
22
HD
21
メインメモリ
30
CMP
10
保管レジスタ
Ksmp
8
保管レジスタ
9
Ksf
復号部
(作業鍵)
Kusr
Permit
Code
Epmp(Ksf)
11
Ksf⊕F(Rei)
=
Kscri
7
暗号処理器
Escr(Di)
Data
12
13
f(Rei)
Di
15
17
キャッシュ
26
CPU
s3
制御ユニット
s1
2
s2
3
18
19
6
スクランブル符号発生器
オフセットレジスタ
4
s4
Address
16
秘密メモリ
5

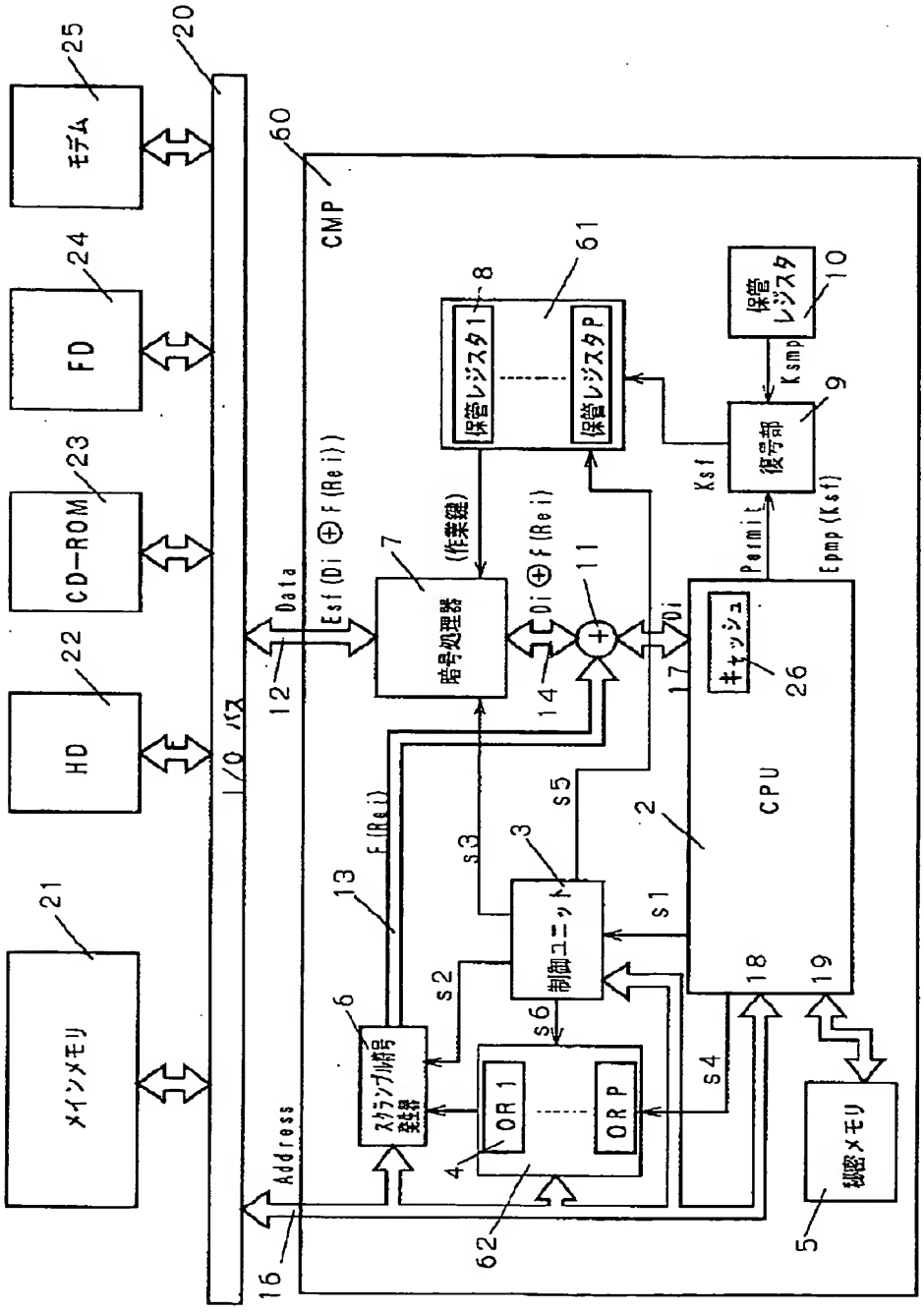
【図１３】


モデム
FD
CD-ROM
HD
メインメモリ
I/O バス
CMP
暗号処理器
保管レジスタ
暗号部
制御ユニット
スクランブル符号生成器
オフセットレジスタ
CPU
キャッシュ
秘密メモリ
Data
Address
Essss(Di ⊕ F(Rei))
Di ⊕ F(Rei)
(作業鍵)
Ksss=Essp(Kusu)
Kssp
Kusr
F(Rei)
Di
s1
s2
s3
s4
20
21
22
23
24
25
26
40
41

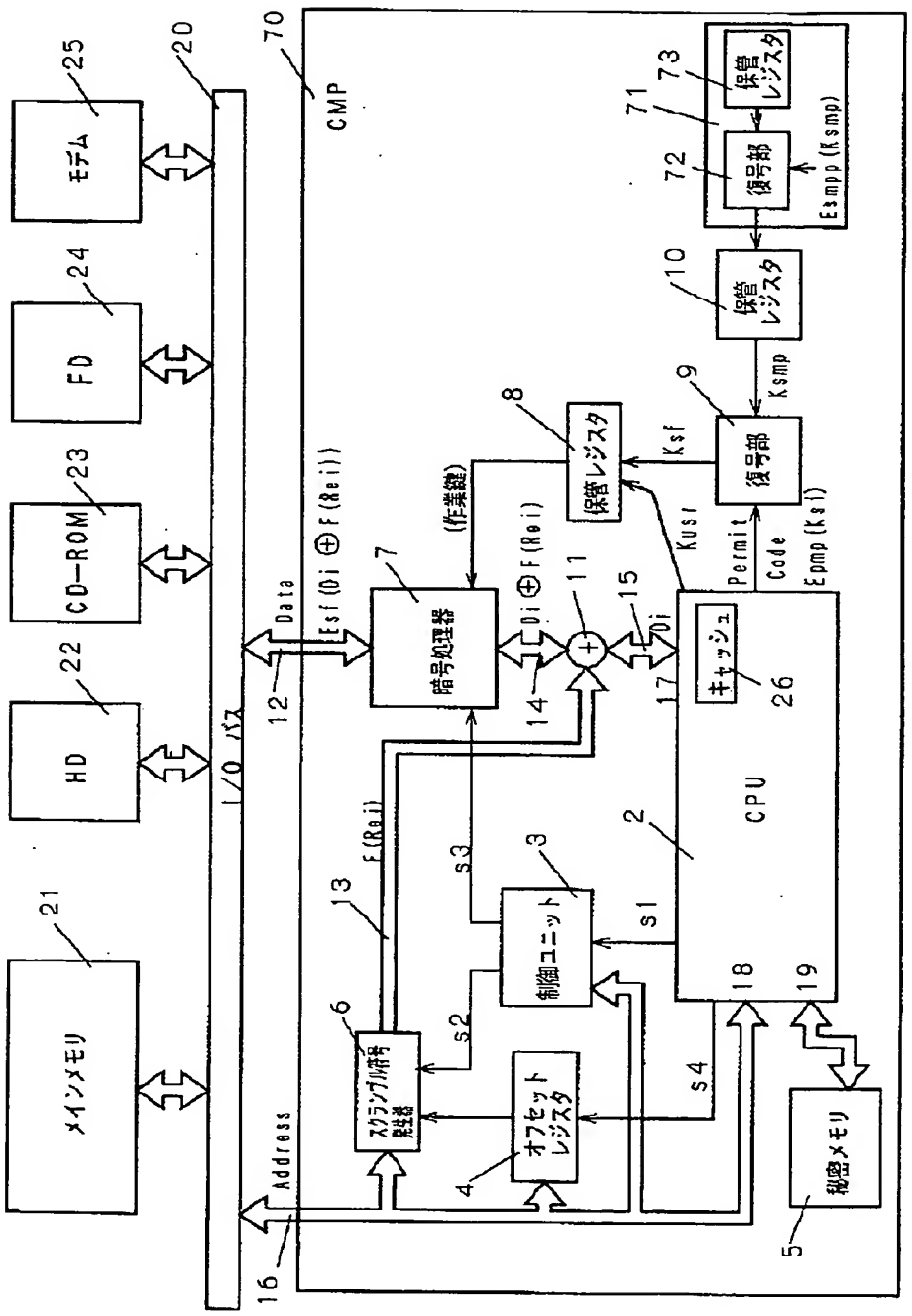
【図１４】


モデム
FD
CD-ROM
HD
メインメモリ
I/O バス
CMP
CPU
暗号処理器
制御ユニット
スクランブル符号発生器
オフセットレジスタ
保管レジスタ
復号部
キャッシュ
秘密メモリ部
照合手段
Data
Address
Esf(Di ⊕ F(Rei))
Di ⊕ F(Rei)
F(Rei)
(作業鍵)
Ksf
Ksm
Kusr
Permit
Code
Epmp(Ksf)
s1
s2
s3
s4
Di
20
21
22
23
24
25
50
51
52

【図１５】


モデム
FD
CD-ROM
HD
メインメモリ
I/O バス
CMP
CPU
暗号処理器
制御ユニット
キャッシュ
復号部
保管レジスタ
保管レジスタ1
保管レジスタP
スクランブル解除登録
OR 1
OR P
秘密メモリ
Data
Address
Esf (Di ⊕ f (Rei))
Di ⊕ f (Rei)
f (Rei)
(作業鍵)
Ksf
Ksmp
Permit
Epmp (Ksf)
Di
s1
s2
s3
s4
s5
s6

【図１６】




フロントページの続き

| (51) Int. Cl. ⁶ | 識別記号 | FI | |
|---|---|---|---|
| H04L 9/14 | | H04L 9/00 | 641 |
| 9/32 | | | 673A |